UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,757	04/28/2006	Pim Theo Tuyls	NL 031322	6967

24737 7590 08/17/2009

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
08/17/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/577,757	TUYLS ET AL.	
	Examiner	Art Unit	
	NADIA KHOSHNOODI	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 April 2006* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

The listing of references in the Search Report is not considered to be an information disclosure statement (IDS) complying with 37 CFR 1.98. 37 CFR 1.98(a)(2) requires a legible copy of: (1) each foreign patent; (2) each publication or that portion which caused it to be listed; (3) for each cited pending U.S. application, the application specification including claims, and any drawing of the application, or that portion of the application which caused it to be listed including any claims directed to that portion, unless the cited pending U.S. application is stored in the Image File Wrapper (IFW) system; and (4) all other information, or that portion which caused it to be listed. In addition, each IDS must include a list of all patents, publications, applications, or other information submitted for consideration by the Office (see 37 CFR 1.98(a)(1) and (b)), and MPEP § 609.04(a), subsection I. states, "the list ... must be submitted on a separate paper." Therefore, the references cited in the Search Report have not been considered. Applicant is advised that the date of submission of any item of information or any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the IDS, including all "statement" requirements of 37 CFR 1.97(e). See MPEP § 609.05(a).

The listing of references in the specification is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, or other information submitted for consideration by the Office, and MPEP § 609.04(a) states, "the list may not be incorporated into the specification but must be submitted in a separate paper." Therefore, unless

the references have been cited by the examiner on form PTO-892, they have not been considered. Specifically, Applicants cite US Patent No. 6,772,339 in the Specification on page 1, line 25 and NPL titled "Cryptography with Rationals" (in Financial Cryptography 2001) on page 14, lines 8-9 of the Specification. Applicants are required to submit a proper IDS citing the references listed in the Specification and are also required to submit a copy of the NPL to the Office for review.

Specification

The abstract of the disclosure is objected to because the abstract filed is not in proper form. According to the MPEP § 608.01(b), "the abstract must commence on a separate physical sheet or electronic page." Instead, Applicants filed the first page of the corresponding PCT (WO 2005/043808) as the abstract, where this is not sufficient. Correction is required.

Drawings

The drawings are objected to because descriptive labels other than numerical are needed for figures 1-2. See 37 CFR 1.84(o). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

I. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

II. Claims 1-7 and 9 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter, as they do not fall under any of the statutory classes of inventions. The language in the claims raise an issue because the claims are directed merely to an abstract idea that is not tied to an article of manufacture which would result in a practical application to form the basis of statutory subject matter under 35 U.S.C. 101.

Claims 1-7 are rejected under 35 U.S.C. 101 based on Supreme Court precedent and recent Federal Circuit decisions, a 35 U.S.C § 101 process must (1) be tied to a particular machine or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In re Bilski et al, 88 USPQ 2d 1385 CAFC (2008); Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584, 588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S. 780,787-88 (1876).

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory process, the claim should positively recite the particular machine to which it is tied, for example by identifying the apparatus that accomplishes the method steps, or positively recite the subject matter that is being transformed, for example by identifying the material that is being changed to a different state.

Here, it is unclear if the "***party (100)***" (since not explicitly described in the specification as being a hardware component) is intended to be the particular machine that the steps are tied to. Although there may be support for the "***party (100)***" to be a hardware element in the

Specification, Examiner requests clarification because the Examiner cannot merely presume this to be the case. Thus, until further explanation/citations from the Specification supporting that the "***party (100)***" is indeed a hardware element, Applicant's method steps are not tied to a particular machine and do not perform a transformation. Thus, the claims are non-statutory.

The mere recitation of the machine in the preamble with an absence of a machine in the body of the claim fails to make the claim statutory under 35 USC 101. *Note the Board of Patent Appeals Informative Opinion Ex parte Langemyer et al.*

Claim 9 is directed towards a computer program product which is not limited to falling under the statutory classes of invention set forth. Examiner suggests claiming a computer readable storage medium executed on the hardware of the device for it to fall under a statutory class.

Claim Rejections - 35 USC § 112

III. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

IV. Claims 1-9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 1, 8, and 9:

Claims 1, 8, and 9 recite the limitation "second data" in line 10, where previously in line 8 only encrypted second data was introduced. There is insufficient antecedent basis for this limitation in the claim. Since, Applicants included no step to show that the "second encrypted

data" was decrypted prior to its use in line 10 and in order to further treat these claims on their merits, Examiner presumes Applicants intended to refer back to the "second encrypted data" which was previously introduced.

As per claim 2:

A broad range or limitation together with a narrow range or limitation that falls within the broad range or limitation (in the same claim) is considered indefinite, since the resulting claim does not clearly set forth the metes and bounds of the patent protection desired. See MPEP § 2173.05(c). Note the explanation given by the Board of Patent Appeals and Interferences in *Ex parte Wu*, 10 USPQ2d 2031, 2033 (Bd. Pat. App. & Inter. 1989), as to where broad language is followed by "such as" and then narrow language. The Board stated that this can render a claim indefinite by raising a question or doubt as to whether the feature introduced by such language is (a) merely exemplary of the remainder of the claim, and therefore not required, or (b) a required feature of the claims. Note also, for example, the decisions of *Ex parte Steigewald*, 131 USPQ 74 (Bd. App. 1961); *Ex parte Hall*, 83 USPQ 38 (Bd. App. 1948); and *Ex parte Hasche*, 86 USPQ 481 (Bd. App. 1949). In the present instance, claim 1 (where these features are automatically included when referencing claim 2) recites the broad recitation "first data (101), which is either private first data or first data from a two-valued domain," and then claim 2 also recites "wherein the first data is random data from a two-valued domain" which is the narrower statement of the range/limitation. Also, Examiner would like to note that in the instance that the first data was chosen to be "private first data," claim 2 is not clarifying which aspect of the private data is to be modified.

***All other claims are rejected by virtue of their dependency.*

Claim Rejections - 35 USC § 102

V. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

VI. Claims 1-3 and 5-9 are rejected under 35 U.S.C. 102(e) as being fully anticipated by Jakobsson et al., US Patent No. 6,772,339.

As per claims 1, 8, and 9:

Jakobsson et al. teach the method/device/computer program product for a party participating in a secure multiparty multiplication protocol between participants comprising the steps of: the party (100) obtaining first data (101), which is either private first data or first data from a two-valued domain (col. 7, lines 10-16), the party obtaining encrypted second data (102) (col. 7, lines 16-18), the party computing encrypted output data (103) which comprises a randomized encryption of the product of the first data and the second data, using a discrete log based cryptosystem (col. 7, lines 18-22), and the party generating a proof (104) being arranged to show that the encrypted output data is correct (col. 7, line 22 – col. 8, line 24).

As per claim 2:

Jakobsson et al. teach the method according to claim 1. Furthermore, Jakobsson et al. teach wherein the first data is random data from a two-valued domain (col. 6, line 59 - col. 7, line 17).

As per claim 3:

Jakobsson et al. teach the method according to claim 1. Furthermore, Jakobsson et al. teach wherein the discrete log based cryptosystem is the ElGamal cryptosystem (col. 5, lines 4-18).

As per claim 5:

Jakobsson et al. teach the method according to claim 1. Furthermore, Jakobsson et al. teach wherein the protocol further comprises the further step of the party transmitting the proof to at least one of the other participants (col. 7, line 59 - col. 8, line 3).

As per claim 6:

Jakobsson et al. teach the method according to claim 1. Furthermore, Jakobsson et al. teach wherein the protocol comprises the further step of the party transmitting the encrypted output data to at least one of the other participants (col. 8, lines 25-49).

As per claim 7:

Jakobsson et al. teach the method according to claim 1. Furthermore, Jakobsson et al. teach wherein the protocol is executed between two parties (col. 7, lines 10-27).

Claim Rejections - 35 USC § 103

VII. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

VIII. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jakobsson et al., US Patent No. 6,772,339 as applied to claim 1 above, and further in view of Yevgeniy "Introduction to Cryptography."

As per claim 4:

Jakobsson et al. substantially teach the method according to claim 1. Not explicitly disclosed is wherein the encrypted data are Pederson commitments. However, Yevgeniy teaches that the Pederson Commitment can be used to achieve hiding data (pages 8-9 sections 2.5.2 and 2.5.4). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Jakobsson et al. to make use of the Pederson Commitment Scheme to hide the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Yevgeniy suggests how using the Peterson Commitment Scheme results in hiding data on pages 8-9 sections 2.5.2 and 2.5.4.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nadia Khoshnoodi/
Examiner, Art Unit 2437
8/13/2009

NK

/Matthew B Smithers/
Primary Examiner, Art Unit 2437